Enhanced Biometric Recognition for Secure Authentication using Iris Preprocessing and Hyper Elliptic Curve Cryptography

Vani Rajasekar (vanikecit@gmail.com)
kongu engineering college
Premalatha J
kongu engineering college
Sathya K
Kongu Engineering College

Research

Keywords: Biometrics, Iris Authentication, 2D Gabor filter, Hyper Elliptic Curve Cryptography, Recognition Accuracy

Posted Date: February 11th, 2020

DOI: https://doi.org/10.21203/rs.2.23196/v1

Enhanced Biometric Recognition for Secure Authentication using Iris Preprocessing and Hyper Elliptic Curve Cryptography

Vani Rajasekar[1*], J. Premalatha[2], K. Sathya[3]

[1]Dept of CSE, Kongu Engineering college, Perundurai, Erode, India
[2]Dept of IT, Kongu Engineering college, Perundurai, Erode, India
[3]Dept of CT/UG, Kongu Engineering college, Perundurai, Erode, India
[*]vanikecit@gmail.com

Abstract:

Biometrics combined with cryptography can be employed to solve the conceptual and factual identity frauds in digital authentication. Biometric traits are proven to provide enhanced security for detecting crimes because of its interesting features such as accuracy, stability and uniqueness. Although diverse techniques have been raised to address this objective, limitations such as higher computational time, minimal accuracy and maximum recognition time remain. To overcome these challenges an enhanced iris recognition approach has been proposed based on Hyper Elliptic Curve Cryptography (HECC). The proposed study uses 2D Gabor filter approach for perfect feature extraction in iris preprocessing. Light weight cryptographic scheme called HECC was employed to encrypt the iris template to avoid intentional attack by the intruders. The benchmark CASIA Iris V-4 and IITD Iris datasets were used in the proposed approach for experimental analysis. The result analysis witnessed that the prime objective of the research such as lesser false acceptance rate, lesser false rejection rate, maximum accuracy of 99.74%, maximum true acceptance rate of 100%, and minimal recognition time of 3 seconds has been achieved. Also it has been identified that the proposed study outperforms other existing well known techniques.

Key words: Biometrics; Iris Authentication; 2D Gabor filter; Hyper Elliptic Curve Cryptography; Recognition Accuracy.

1. Introduction

With the advancement of information technology, there is a gradual increase in crime and identity fraud. To address the issues related to identity fraud heightened security mechanism is needed. Biometric recognition is the most eminent technology for person authentication in identification systems. Biometric traits accurately determine the identity of a person either by means of their physiological characteristics (finger, iris, hand, face) and behavioral characteristics (gait, signature, voice). One of the most reliable and leading biometric technology is iris recognition system. Iris authentication is most accurate and domain-bounded recognition approach which uses distinctive patterns of human iris. The unique nature of iris is set between lens and cornea of the eye. The iris diameter is about 12 mm and pupil size varies from 10% to 80% of iris. The texture details of iris such as furrows, cornea, filaments, flecks and arching ligaments etc makes iris unique. The unique feature of iris is extracted after proper preprocessing techniques such as localization, normalization, segmentation. The proposed research uses 2D Gabor filter for exact feature extraction from iris.

In addition to the feature extraction of iris, proper encryption is also a major demand. The need for encryption in iris recognition is when original template is stored in database; the intruder may compromise and give access to sensitive data of a user. To overcome these challenges HECC is proposed for encrypting the iris template. HECC is a light weight cryptographic approach [25] that uses very less key size of 80 bits. HECC provides higher security with very less computational time hence it is more suitable for real time applications such as military, E-passport, credit card services, banking applications etc. To address all the security related issues and to obtain an enhanced accuracy, present research work proposes a novel, hybrid iris recognition with HECC encryption [23]. This study shows very less recognition time, less false acceptance and false rejection rate. Till now no applications have been proposed in combination with iris recognition with HECC encryption. The proposed work provides a novel enhanced iris recognition with higher accuracy and less recognition time.

2. Related Works

This section provides the brief overview of various iris recognition and encryption techniques. Aparna et al [9] discussed stable biometric characteristics to recognize a person. Result analysis shows that their scheme shows good performance on CASIA database. Kalka et al [12] used various metrics for iris recognition. Their scheme was based on occlusion, gaze deviation and light reflection based on ICE database. Sun et al [13] specifies iris recognition based on three approaches i.e. coarse iris classification, iris aliveness detection and coarse iris classification. Yongqiang et al [14] proposed a iris recognition model based on global and local iris features. Their scheme uses privacy projection algorithm which converts high dimensional data into lower dimensional data. Vani Rajasekar et al. [15] have proposed an authentication scheme based on signcryption with HECC. It is shown in their work that HECC provides much higher security than other cryptographic algorithms. Zhou et al [17] proposed an enhanced iris recognition model that outperforms the Daugman's model [21]. Their scheme uses snake model and vector field convolution technique to accurately determine the inner edge of the iris. Poursaberi et al [18] proposed an iris recognition approach based on hamming and harmonic mean distance. The dataset used in their method in CASIA V1 and feature extraction method used were wavelet daubechies2. Their observation includes rather than smaller part of iris, more reliable part produces more accuracy.

Galbally et al [19] developed a mechanism that not only for iris authentication but also used for immediate liveliness detection of iris. Burak et al [20] developed an iris recognition system in which the performance greatly depends on coding bits and noise level. Daugman et al [16] used Gaussian filter for segmentation of iris image. Their performance greatly varies due to light illumination and reflections. Neda et al [22] developed a hybrid robust iris recognition approach that uses 2D Gabor filter for feature extraction and neural network, PSO algorithm was employed to improve the generalization performance. Kalka et al uses different metrics for iris recognition such as iris occlusion, amount of reflection and gaze deviation. Their estimation was mainly on the bottom portion of iris and datasets used were ICE, CASIA, and WVU. Ch SA et al developed a signcryption scheme based on HECC. Their analysis shows that encryption using HECC provides much higher security compared to other cryptographic algorithms. Reyes et al [24] focused mainly on the iris texture and variability. Their scheme uses pseudo polar arrangement for matching and biomechanical model to improve the recognition rate and accuracy.

From the observations of above literatures, it has been studied that optimal iris recognition approach can be designed using iris localization, segmentation and normalization. 2D Gabor kernel filter acts as a perfect feature extraction mechanism in iris. There is a need for encryption of original iris template before stored in the database because there is a possibility for an intruder to compromise the template database. The problem identified and literature survey has motivated the research in following ways.

- Iris preprocessing with 2D Gabor filter can be used on normalized iris image for feature extraction.
- A novel approach called HECC can be used for encryption of original iris template as this is a lightweight cryptographic mechanism which provides much higher security in less computational time.
- To design an efficient iris recognition approach with higher accuracy and reduced recognition time.

3. Preliminaries

3.1 HEC and Selection of Genus 2 Curve

For efficient communication to be established among mobile devices, the major requirement is higher security and less power constraints. The existing cryptographic algorithms such as RSA, AES, DES and Elliptic Curve Cryptography have not satisfied such requirements because of its larger key size and complex mathematical calculations involved in encryption and decryption process. HECC is a light weight cryptographic scheme that has lesser key size and provides higher security than the existing schemes. The most attractive feature of HEC is that Genus 2 of HEC is mainly bounded on finite fields and algebraic geometry. Let S be a finite field and $\bar{S}$ be algebraic closure of S. The HEC with genus 2 over S is given by

$$Curve, C : f(x) = y^2 + h(x)y \text{ in S[x,y]} \qquad (1)$$

Where, h(x) ε S(x) defined as polynomial of degree g and f(x) denotes a monic polynomial of degree 2g+1. The most important point in HEC is choosing of appropriate curve for application. The proposed research work uses a method called Extended Complex Multiplication (ECM) over P (prime field) and length of p is 64 bits. Hence the time taken for executing brute force attack by the attacker in the proposed system will be much higher than the time taken for cryptanalysis.

3.2 Selection of genus 2 group elements and group operations

The group elements of HEC is not a rational point as in case of Elliptic curve instead a divisor. In proposed research work, a divisor of HEC is identified by combining certain number of points using a technique called

Mumford representation. Generally HECC allows addictive group which involves divisor addition, divisor doubling and divisor inversion. The proposed research uses a technique called Cantor algorithm for divisor addition and divisor Inversion.

3.3 Dataset used:

There are two datasets used in the proposed research work. One of which is Chinese Academy of Science and Institute of Automation (CASIA) Iris Image Database Version 4.0 [10]. This dataset is an extension of CASIA Iris Image Database Version 3.0. The dataset contains 54,600 iris images captured from 2,800 distinct subjects. All images are jpeg files of 8 bit grey scale. One of the subset of CASIA V4 is Iris Thousand image dataset which contains 20,000 high quality iris images. Another dataset used in this research is Indian Institute of Technology Delhi (IITD) iris image dataset [1]. This contains about 2240 iris image acquired from 224 different users of age group 14-55 years comprising of 176 males and 48 females. The resolution of these images is 320X240 pixels. Because of this high resolution both the datasets are well suited for analysis of real time biometric authentication models.

4. Proposed Methodology

Iris is a unique physiological biometric trait of a person that can be used for authentication in many applications. The proposed study employs iris preprocessing as the initial step. The preprocessed 64 bit original noise removed templates are converted to cipher templates using encryption in HECC approach and all obtained cipher templates are stored in the database. For authentication, one of the test iris image from the database is taken and it is preprocessed, cipher templates are created using HECC. The resultant cipher template is compared with the one stored in the database using Euclidean distance (ED). ED is used to compare the cipher templates in database with the cipher template of test iris given in equation (2). If the comparison meets the threshold value biometric authentication success else authentication fails and procedure will be terminated. The overall block diagram of proposed methodology is specified in Fig.1.

$$D(s,t) = \sqrt{\sum_{i=1}^{n} \left(s_i - t_i\right)^2} \qquad (2)$$

Where s_i is cipher template stored in database

t_i is cipher template of test iris image

4.1. Iris Pre processing

High quality of iris image acquisition generally results in higher accuracy for any authentication procedure. The Iris image pre processing consists of two phases. 1. Iris localization 2.Iris Normalization. These were performed to identify the ROI (Region of Interest) of iris and also to minimize the noise present in iris image.

A) Iris Localization:

This procedure detects the border internally and externally without error that separates the Sclera and Pupil part of iris. The proposed work uses Circular Hough Transform Algorithm (CHTA) for localization. The grey scale format can be applied to the captured image. In iris the region where dim pixels surrounded by light pixels are known as holes. An edge detection operator known as canny edge detector is used to locate the edge map on gray image. The CHTA is applied on the specific areas to perfectly identify the inner and outer circle iris parameters given in Fig.2. b).

B) Iris Normalization:

Conversion of iris image in Cartesian products to polar coordinates is called normalization. The proposed work used Daugman's Rubber Sheet model for normalization shown in Fig.3. Here the ring of iris image is transformed to rectangular projection of size (64X512). The images of iris area are I(X,Y), Cartesian coordinates are (X,Y), polar coordinates are specified as (r,θ), (X1,Y1) and (X2,Y2) represents the iris and pupil boundaries in θ direction.

$$I\left(X\left(r,\theta\right),Y\left(r,\theta\right)\right) \rightarrow I\left(r,\theta\right) \qquad (3)$$

$$X\left(r,\theta\right) = (1-r)X2(\theta) + rX1(\theta) \qquad (4)$$

$$Y\left(r,\theta\right) = (1-r)Y2(\theta) + rY1(\theta) \qquad (5)$$

C) Iris Segmentation:

Segmentation is considered to be the most important step in iris pre processing given in Fig.2 c). The proposed work uses centroid and bounding box method to identify the center and radius of located pupil. To fix the lower and upper column in both horizontal and vertical direction, the center coordinate value of pupil is added to and subtracted from radius respectively. The iris part is segmented to 50 pixels from either side of pupil boundary to generate iris template based on CASIA Iris dataset [11].

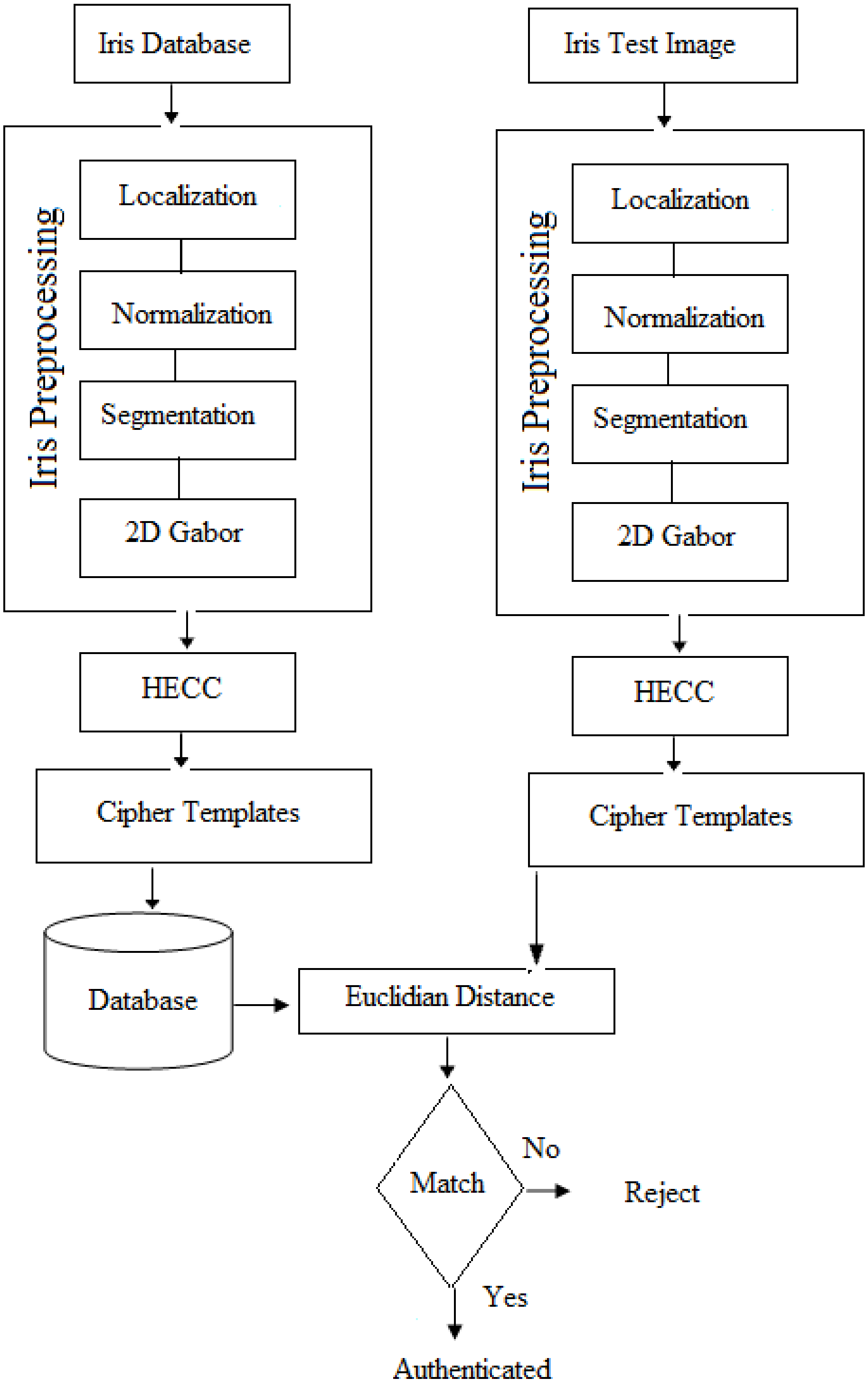

Fig.1. Block Diagram of Proposed Methodology

D) 2D Gabor Kernel Filter:

2D Gabor Kernel filter is the excellent feature extraction mechanism of iris. The more prominent features of this filter are the decomposition of input image into various images based on their textural information. A Gabor filter bank was employed to explain the channels present in frequency domain and spatial domain simultaneously. The filter parameters are precisely chosen for the determination of human visualization. The superfluous nature of Gabor filter reduces the feature dimension. The Gabor kernel approach was chosen in which each trained samples are twisted with the other Gabor channels. The distance between and within the gabor channels are calculated. The 2D Gabor filter representation in spatial domain are given as

$$G\lambda\psi\theta\Omega\gamma(X,Y)=\exp\left(-\frac{X'^2+\gamma^2 Y'^2}{2\Omega^2}\right)\cos\left(2\Pi\frac{X'}{\lambda}+\psi\right) \qquad (6)$$

Where

$$X'=X\cos(\theta)+Y\sin(\theta) \qquad (7)$$

$$Y'=Y\cos(\theta)-X\sin(\theta) \qquad (8)$$

In equation (5) λ is the sinusoidal function wavelength, θ is the orientation of Gabor filter, ψ is the offset of Gabor filter, Ω is the bandwidth and γ is the aspect ratio.

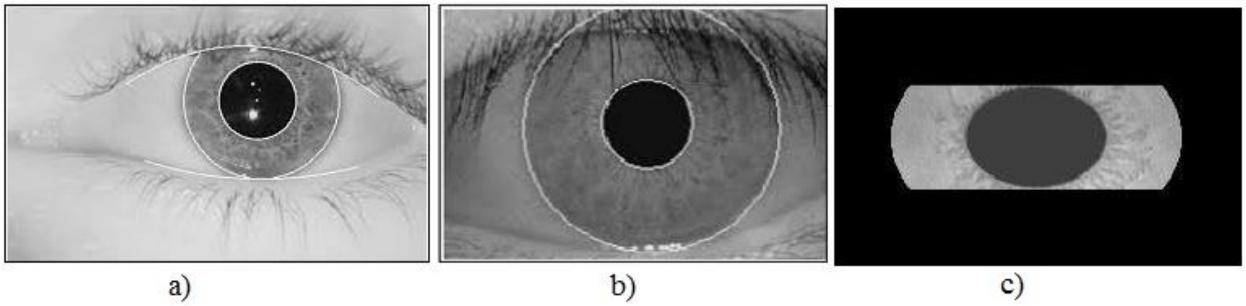

Fig.2. Iris Preprocessing: a) Original Iris b) Iris Localization c) Iris Segmentation

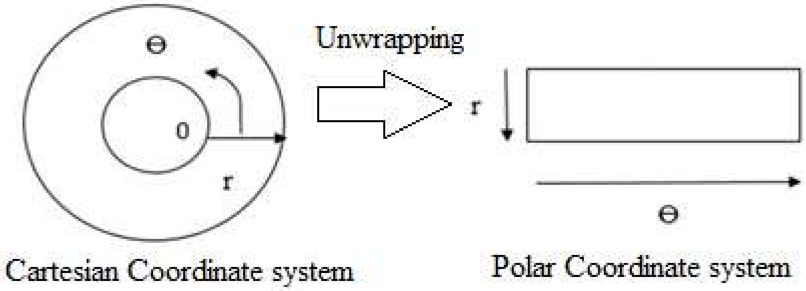

Fig.3. Daugman's Rubber Sheet Model

4.2 Hyper Elliptic Curve Cryptographic approach

The steps involved in HECC approach are a) Extended Complex Multiplication (ECM) to select the proper genus 2 HEC with cardinality N. b) Restricted Iris Template (RIT) to reduce the template size within 64 bits. c) Point to Divisor Conversion (PDC) algorithm to convert HEC points to Divisors which is based on Mumford representation. Once the divisors are generated the next step is d) Randomized Construction of Divisors (RCD) to generate random divisor which then combines with sequence of divisors from step c) forms the Cipher Divisors by the procedure Divisor Addition based on Cantor Algorithm (DACA). e) Cipher Divisors are converted to Cipher points using the algorithm Divisor to Point Conversion (DPC). The cipher templates are retrieved from cipher points as this is the final step in HECC approach. The cipher templates are stored in database. The block diagram of HECC approach is shown in Fig.4 and entire step involved in encryption is specified in algorithm 7 (Iris Template Encryption) ITE.

4.2.1. Designing of HEC using ECM

The security of the proposed system can be enhanced by concept of Discrete Logarithmic Problem (DLP) of HEC. This denotes the selection of suitable prime number of size 64 bits and group order should be the product of this 64 bit prime number. The curve selection of HEC based on ECM is given in algorithm 1. The proposed system is designed to have iris image of size 64 bits. The genus 2 HEC must generate to include all possible binary sequence of size 64 bits. As HEC is based on genus-2 over GF (P), it may not be possible to generate all sequence of 64 bits. Hence iris segmented image after 2D Gabor filter applied is restricted to generate the points within the prime field which is depicted in algorithm 2.

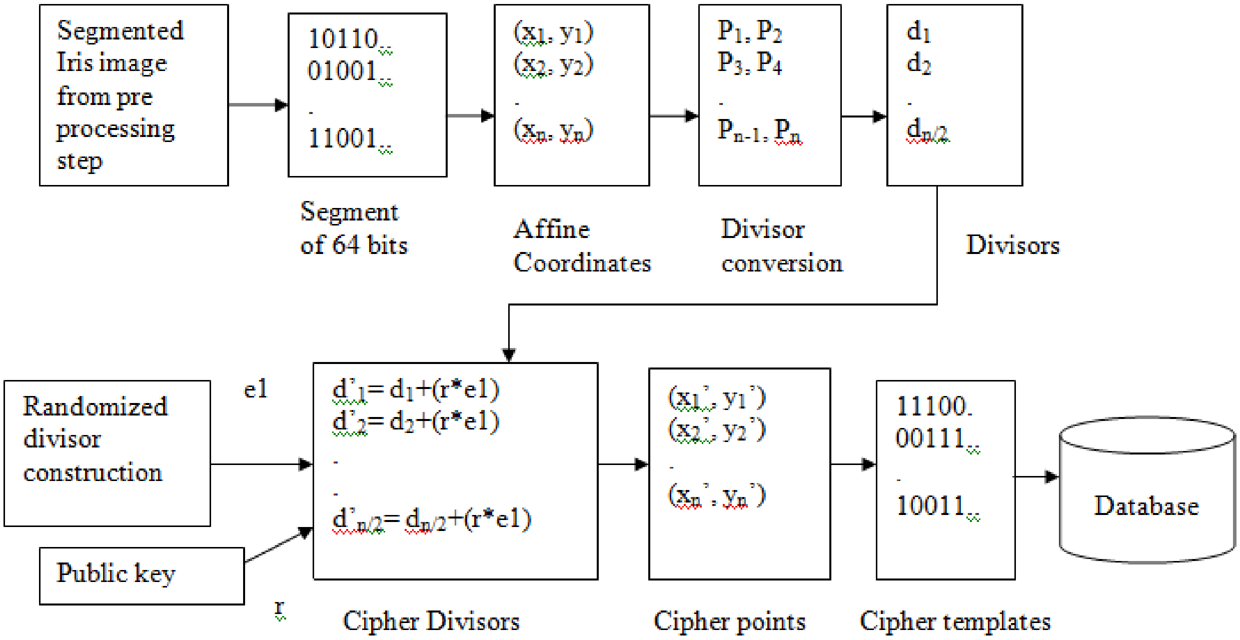

Fig.4. Hyper Elliptic Curve Cryptographic approach

Algorithm 1: Extended Complex Multiplication (ECM)

```
Input: 64 bit large prime number
Output: HEC of Genus-2 with larger cardinality N
Process:
While true do
Repeat
Repeat choose p=64 bits
Until factoring of $p = \varpi * \omega$ as prime ideals
Calculate all probable cardinality N
Until one satisfies cardinality N
For s=1,2,3 then p=4s+3 where $s \in N$
Compute roots as $J_s = \{J_s^{(i)}\}$
Where $(j_1, j_2, j_3) \in (J_1, J_2, J_3)$
Compute conic $\theta_{j_1, j_2, j_3}(x_1, x_2, x_3)$
If a point $(A_1, A_2, A_3)$ lies with $\theta_{j_1, j_2, j_3}(x_1, x_2, x_3)$=0 then
Calculate $h_{j_1, j_2, j_3}$ and intersecting polynomial
If intersecting polynomial contain a root in $F_p$ then
```

```
Locate Genus-2 HEC
Identify the random divisor
Compute cardinality N
If N is seems to be preferred
Break and return Curve C and cardinality N
```

Algorithm 2: Restricted Iris Template (RIT)

```
Input: 64 bit Iris template
Output:  Iris template within 64 bits
Process:
For each sample, $T_i$ do
$T'_i = \left(T_i \times \left(2^{-1}\right) \bmod p\right) \bmod p$
```

4.2.2 HEC points and HEC Divisors

HEC with genus 2 over 2g+1 is given in equation (1) and all non trivial elements in HEC are specified as divisors. The divisors are symbolized with the monic polynomials u(x) and v(x). It is based on three conditions a) u is monic b) Degree of v should be less than degree of u c) degree of u and v < genus-2. The group operation of HEC is based on divisors hence there is a need for conversion of HEC points to Divisors and Divisors to HEC points. And because of group property HECC it is faster than Elliptic Curve Cryptography (ECC). Hence, HECC is well suited for Light weight cryptographic applications. Algorithm 3 represents the conversion of HEC points to divisors. The divisor of HEC based on Mumford representation with two pair of polynomials u and v.

$$u\left(X\right) = X^{2} + A * X + B \tag{9}$$

$$v\left(X\right) = C * X + D \tag{10}$$

Algorithm 3: Point to Divisor Conversion (PDC)

```
Input: p1(a1,b1), p2(a2,b2)
Output: $d = \left(X^{2} + A * X + B, C * X + D\right) \bmod p$
Process:
Compute the following
1. $A = \left(-a1 - a2\right) \bmod p$
2. $B = \left(a1 * a2\right) \bmod p$
Solve C and D as follows
1. $C * a1 + D = b1$
2. $C * a2 + D = b2$
Return divisor as $d = \left(X^{2} + A * X + B, C * X + D\right) \bmod p$
```

4.2.3 Randomized Divisor Construction:

The proposed biometric crypto system is a non deterministic one in which for the same iris and key pair it produces different cipher template every time. It is the most desirable property of the proposed system as it eliminates the known cipher text attack. Therefore there is a need to construct randomized divisor every time and it is specified in algorithm 4.

Algorithm 4: Randomized Construction of Divisors (RCD)

```
Input: p prime number and HEC curve C
Output: Randomized divisor e1
Process:
While true do
```

```
Let a1, a2 be the two numbers such that $a1,a2 \in \{1,2,3,..p-1\}$
Calculate $S1=\sqrt{f(a1)\bmod p}$
Calculate $S2=\sqrt{f(a2)\bmod p}$
Where f(a1) and f(a2) are curve functions
If $\left(S1^{2}\bmod p == f(a1)\bmod p\right)\&\&\left(S2^{2}\bmod p == f(a2)\bmod p\right)$
p1= (a1,S1) and p2= (a2,S2) are valid points
Form divisor e1 using algorithm PDC with points p1 and p2, break
Return randomized divisor e1.
```

4.2.4 Divisor Grouping:

The divisor grouping in HEC is based on Cantor algorithm. This algorithm takes two randomized divisor as input and produces unique divisor. As hyper elliptic operation is generally based on additive group, the necessary method for proposed cryptosystem is Divisor Addition in template encryption. Algorithm 5 depicts the steps involved in Divisor Addition.

Algorithm 5: Divisor Addition based on Cantor Algorithm (DACA)

```
Input: Divisors d1=[a1,b1], d2=[a2,b2]
Output: d=d1+d2
Process:
Calculate
    S1=gcd(a1,a2)
    S1=e1a1+e2a2
Compute
    D=gcd(S1,b1+b2+h)
    D=C1S1+C2(b1+b2+h)
Calculate t1=C1e1, t2=C1e2, t3=C2
Compute $u=\frac{a1a2}{D^{2}}$
Compute $v=\frac{t1a1b2+t2a2b1+t3(b1b2+f)}{D}\bmod u$
Repeat
Calculate $t'=\frac{f-hv-v^{2}}{u}$, $k'=(-v-h)\bmod t'$
$u=t',v=k'$
Until deg(u)<=g
Make u as a monic
Return cipher divisor as d'[u,v]
```

4.2.5 Iris Template encryption:

The main question of template encryption in the proposed scheme is to avoid the eavesdropping of sensitive data by the attacker or sometimes the compromising of original template database by the attacker. One possible solution for this challenge is to ensure the privacy preserving of biometric template by means of cryptographic primitives. The direct employment of such cryptographic primitive is encryption of biometric template using HECC. The cipher divisors are converted to cipher points using the algorithm 6 DPC. The proposed encryption method converts the original iris template into cipher iris template. The steps involved in the proposed encryption are depicted in algorithm 7.

Algorithm 6: Divisor to Point Conversion (DPC)

```
Input: $d = \left(X^{2} + A*X + B, C*X + D\right) \bmod p$
Output: p1(a1,b1), p2(a2,b2)
Process:
Calculate
$X^{2} + A*X = -b \bmod p$
$(X + A*(2^{-1} \bmod p))^{2} \bmod p = -b - A*(2^{-1} \bmod p) \bmod p$
$(X + A*(2^{-1} \bmod p))\ \ \bmod p = sqrt \bmod p(-b - A*(2^{-1} \bmod p) \bmod p)$
Compute
$X1 = (sqrtm\left(-b*\left(2^{-1} \bmod p\right)\right) - A*\left(2^{-1} \bmod p\right)) \bmod p$
$X2 = (-sqrtm\left(-b*\left(2^{-1} \bmod p\right)\right) - A*\left(2^{-1} \bmod p\right)) \bmod p$
Calculate
$Y1 = v(X1)$
$Y2 = v(X2)$
Return $(X1, Y1) and (X2, Y2)$
```

Algorithm 7: Proposed Iris Template Encryption (ITE)

```
Input: Original iris template I
Output: Encrypted iris template I'
Process:
Choose genus 2 HEC using ECM
Convert original iris template to points in HEC
Convert all the points of HEC to divisors using PDC
Select random divisor e11 based on algorithm RCD
Select public key $r \in \{2,3,4..p-1\}$
For each 4 consecutive samples (I1, I2, I3, I4) do
Form randomized divisor e1 using algorithm RCD
Calculate $d'_{i} = d + (r*e1)$ using DACA
Return all computed cipher divisors $d'_{i}$.
Convert cipher divisors to cipher points using DPC
Convert cipher points to cipher template
Store cipher template in database
```

5. Results and Discussion

The proposed method is implemented in Anaconda 3 (Spyder) using Python programming language with the system having i5 processor and 8 GB RAM. The experimental set up of proposed method is divided into training set and test set. From the two datasets CASIA and IITD iris, 9 images were taken for training and one image is used for testing. The following five metrics are considered for determining the effectiveness of the proposed research. They are False Acceptance Rate (FAR), False Rejection Rate (FRR), True Acceptance Rate (TAR), Equal Error Rate (EER) and Accuracy.

- False Acceptance Rate (FAR): It is the probability in which the biometric system fallaciously accepts the unauthorized user. It happens when biometric system inaccurately matches the cipher template of user with the stored cipher template in database.
- False Rejection Rate (FRR): It is the probability in which the biometric system denies access to the authorized user. It happens when biometric system fails to match the cipher template of user with the stored cipher template in database.
- True Acceptance Rate (TAR): It is the probability in which the biometric system correctly identifies the authorized user.

- Equal Error Rate (EER): The Rate in which FAR is equal to FRR is known as ERR
- Accuracy: Refers to number of legitimate users granted access to the number of attempts for authentication

5.1. Performance evaluation of proposed method on CASIA Iris Thousand dataset

To understand the feasibility of proposed method, 50 persons iris samples from CASIA Iris Thousand dataset are taken and parameters such as FAR, FRR, ERR, TAR and accuracy are computed for variation of threshold values as shown in Table 1. From the analysis it is witnessed that the proposed method has maximum TAR of 100% and optimum TAR of 90%. The average EER in the proposed method on CASIA dataset is 10% at threshold 0.70. The graphical representation of performance metrics is specified in the Fig 5 and Fig 6.

Table 1. Performance evaluation with varying thresholds on CASIA dataset

	50 Iris Samples			**100 Iris Samples**		
Threshold	**FAR**	**FRR**	**TAR**	**FAR**	**FRR**	**TAR**
0.45	0	50	0	0	100	0
0.50	0	47	6	0	97	3
0.55	0	40	20	0	89	11
0.60	0	32	36	0	52	48
0.65	0	25	50	0	30	70
0.70	4	4	92	12	12	88
0.75	17	3	94	50	7	93
0.80	39	1	98	84	2	99
0.85	50	0	100	92	0	100

5.2. Performance evaluation of proposed method on IITD Iris dataset

To understand the feasibility of proposed method, 50 persons iris samples from IITD Iris dataset are taken and parameters such as FAR, FRR, ERR, TAR and accuracy are computed for variation of threshold values as shown in Table 2. From the analysis on IITD iris data it is inferred that the proposed method have maximum TAR of 100%. The EER of 11% is identified at the threshold 0.70 with optimum TAR of 89%. The graphical representation of performance metrics is specified in the Fig 7 and Fig 8.

Table 2. Performance evaluation with varying thresholds on IITD iris dataset

	50 Iris Samples			**100 Iris Samples**		
Threshold	**FAR**	**FRR**	**TAR**	**FAR**	**FRR**	**TAR**
0.45	0	50	0	0	100	0
0.50	0	44	12	0	93	7
0.55	0	36	28	0	79	21
0.60	0	22	56	0	52	48
0.65	0	19	62	0	38	62
0.70	5	5	90	13	13	87
0.75	19	1	98	37	7	93
0.80	36	0	99	63	0	99
0.85	50	0	100	97	0	100

5.3. Comparison of accuracy and maximum TAR of proposed method with existing methods

The table 3 shows the EER, maximum TAR, optimum TAR and accuracy of proposed method on both CASIA Iris and IITD Iris dataset. The comparison also shows the recognition time of proposed method in seconds. The performance metrics of the proposed scheme is compared with the existing scheme in terms of accuracy and maximum TAR as shown in table 4.

Table 3. Performance parameters of proposed method on both iris dataset

Dataset used	**EER**	**Maximum TAR**	**Optimum TAR**	**Accuracy**	**Recognition Time (sec)**
CASIA Iris Thousand	10%	100%	90%	99.78%	3s
IITD Iris	11%	100%	89%	99.7%	3 s

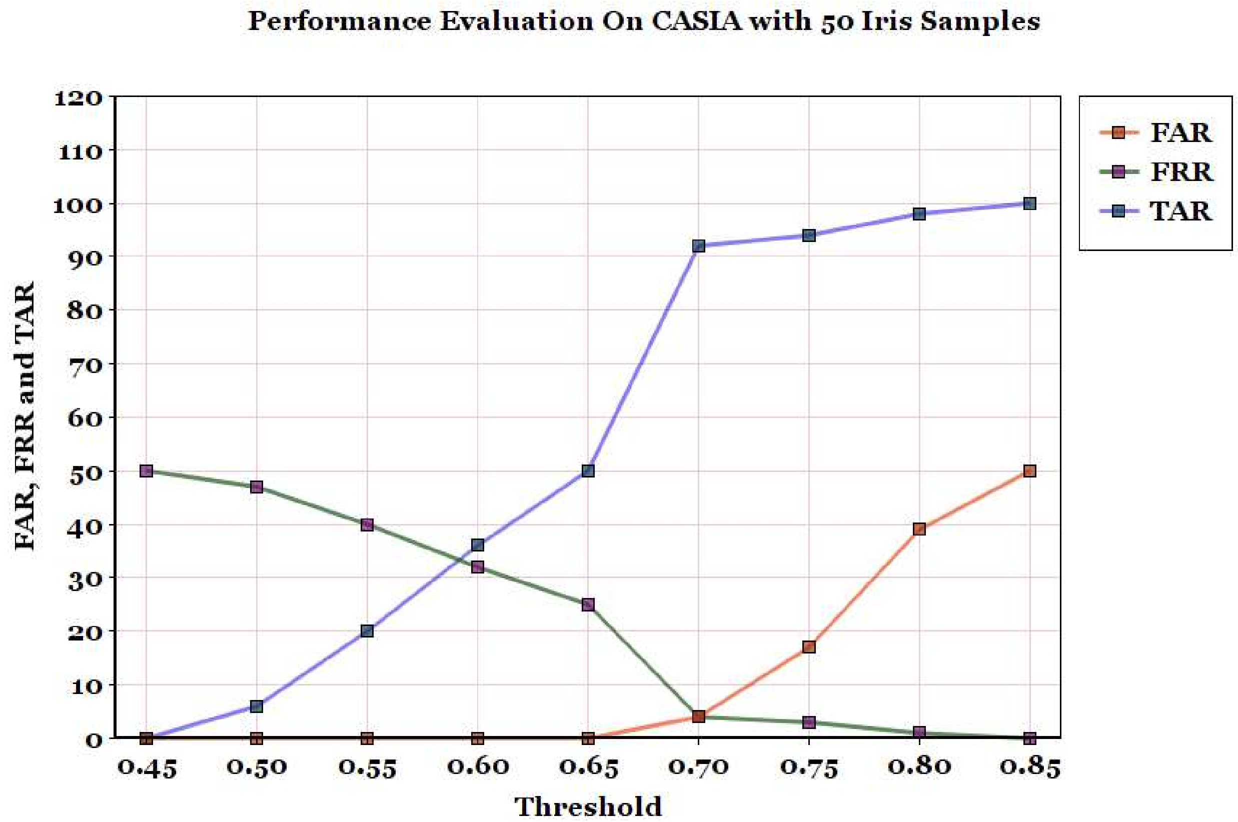

Fig. 5. Plot of FAR, FRR and TAR with varying threshold on CASIA dataset with 50 Iris images

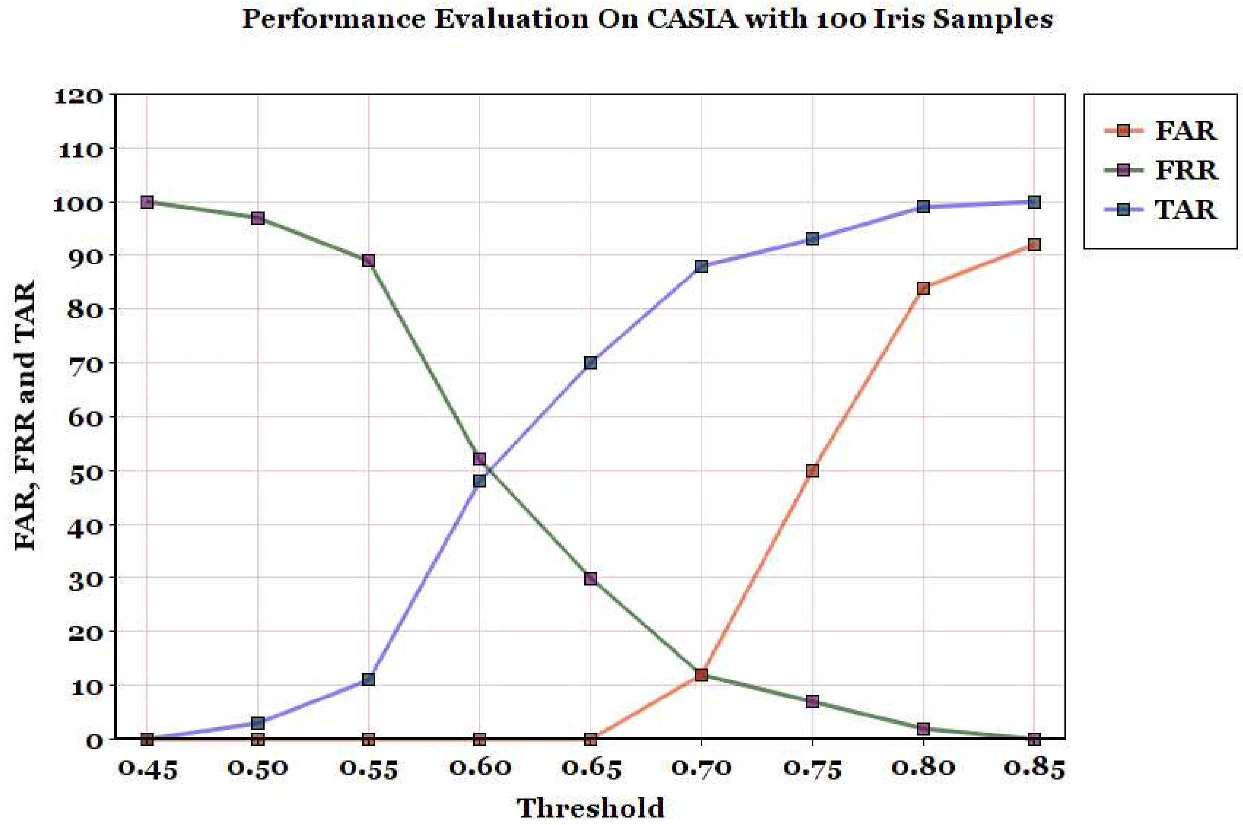

Fig. 6. Plot of FAR, FRR and TAR with varying threshold on CASIA dataset with 100 Iris images

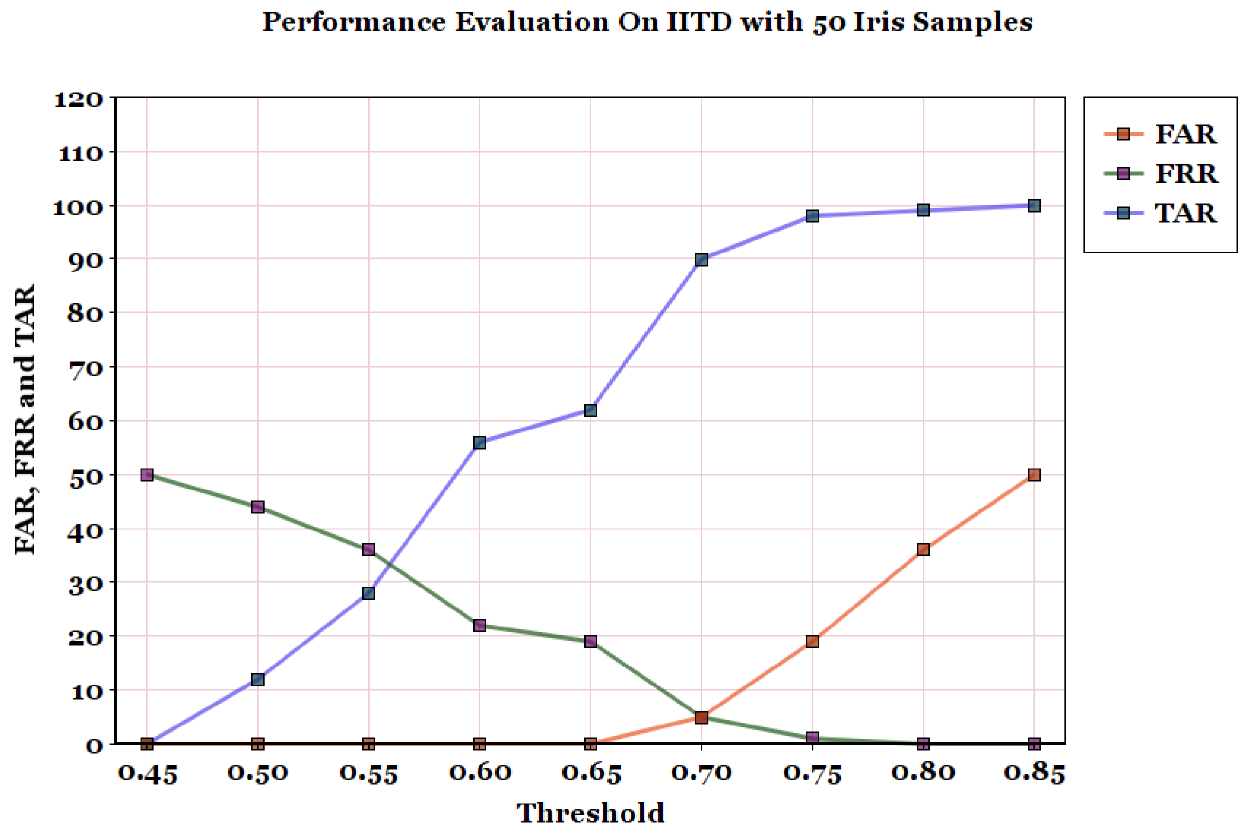

Fig. 7. Plot of FAR, FRR and TAR with varying threshold on IITD dataset with 50 Iris images

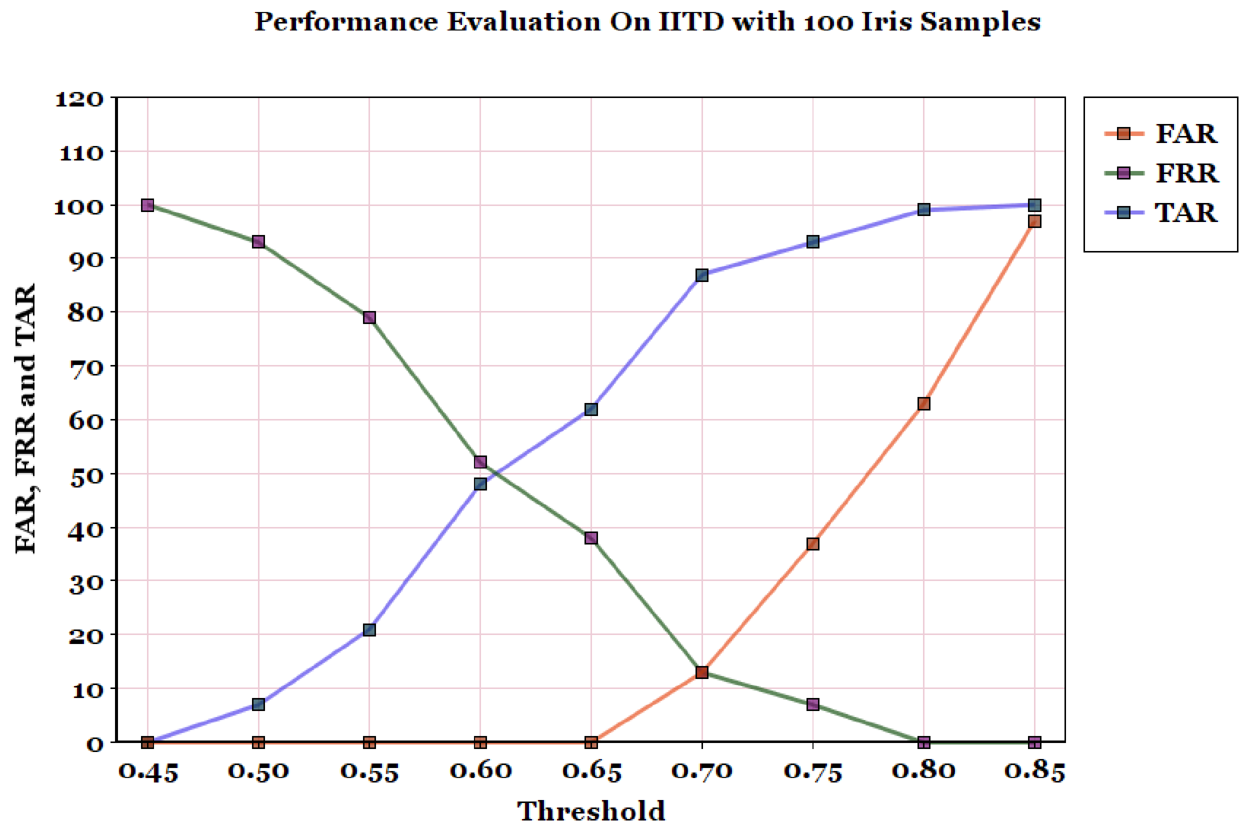

Fig. 8. Plot of FAR, FRR and TAR with varying threshold on IITD dataset with 100 Iris images

Table 4. Accuracy and maximum TAR of proposed and existing authentication schemes

Methods	**Dataset used**	**Algorithm used**	**Maximum TAR**	**Accuracy**
Deepanshu kumar et al. [7]	MMU	DWT+DCT	75.59%	80%
N.L. Manasa et al.	CASIA	LBP score level fusion	97%	98.2%
Mohamed Abdolahi et al. [3]	CASIA	Fuzzy logic	93%	97.5%
Gayathri et al [2]	IITK iris	Fusion technique	87%	99.2%
Velmurugan et al. [4]	CASIA and IITD Iris	DCT wavelet Technique	91%	99.4%
Fernando et al [5]	CASIA Internal v-3	2-D Gabor	99.8%	99%
Mohamed Hamaz Abed [6]	CHUK iris	DWT and Cosine	99.25%	98%
Serestina et al [8]	CASIA and UBIRIS	Vote based strategies	96%	99.6%
Proposed Iris Recognition	**CASIA and IITD Iris**	**2D Gabor + HECC**	**100%**	**99.74%**

6. Conclusion and Future work

The proposed study presented a two novel approach such as 2D gabor kernel for feature extraction and HECC approach for encrypting original iris template to cipher templates. The major need of encrypting the iris template is to avoid the compromising of template database by the attacker. The research has been implemented on CASIA Iris V4 and IITD iris dataset. More attention has been given on evaluating the efficiency of the proposed algorithm. The result analysis witnessed that the proposed research has maximum TAR of 100%, accuracy of 99.74% with very less recognition time of 3 seconds. The method also outperforms the existing iris authentication techniques by means of accuracy and maximum TAR. Because of such higher accuracy and security the proposed study will find it applications in Military applications, Border control applications, Banking, Aadhar etc. Future work will investigate on implementing signcryption technique in iris recognition so as to improve accuracy and security in much better way.

7. List of Abbreviations

HECC - Hyper Elliptic Curve Cryptography
` ECM - Extended Complex Multiplication
CASIA- Chinese Academy of Science and Institute of Automation
IITD- Indian Institute of Technology Delhi
CHTA- Circular Hough Transform Algorithm
RIT - Restricted Iris Template
PDC- Point to Divisor Conversion
RDC-Randomized Construction of Divisors
DACA-Divisor Addition based on Cantor Algorithm
DPC-Divisor to Point Conversion
ITE-Iris Template Encryption
FAR- False Acceptance Rate
FRR- False Rejection Rate
TAR-True Acceptance Rate
ERR- Equal Error Rate

8. Declarations

Availability of supporting data

No supporting data is associated in this research

Conflicts of Interest

The authors declare here that they have no conflict of interest.

Data Availability Statement

The dataset used for experimental analysis are CASIA Iris V-4 and IITD Dataset which is publically available.

Funding Statement

The authors declare here that no funding has been got for this research work

Authors' contributions

Vani Rajasekar have prepared and experimented the research
Dr.J.Premalatha have made proof read and verified
Sathya K helped in collecting data sets and made proof read

Authors' information

Vani Rajasekar completed her B.Tech(IT), M.Tech (Information and cyberwarefare) in department of IT Kongu engineering college. She is pursuing her PhD (Information and Communication Engineering) in the area of Network security. Presently she is working as assistant professor in the department of CSE Kongu engineering college for past 3 years. Her area of interest includes Network security, Cryptography and Wireless networks.

Dr.J.Premalatha completed BE(ECE), ME(CSE), PhD(Information and Communication Engineering). She is working as professor in the department of IT Kongu engineering college. Her teaching experience is 28 years. Her area of interest includes Network security, Cryptography, Computer networks and Database Management system.

K.Sathya completed her B.Tech(IT), M.Tech (Information and cyberwarefare) in dept of IT Kongu engineering college. She is pursuing her PhD (Information and Communication Engineering) in the area of Network security. Presently she is working as assistant professor in the department of CT/UG Kongu engineering college for past 3 years. Her area of interest includes Network security, Computer networks.

References:

[1] Ajay Kumar and Arun Passi, "Comparison and combination of iris matchers for reliable personal identification," Proc. CVPR 2008, Anchorage, Alaska, pp. 21-27 Jun. 2008

[2] Gayathri R and Ramamoorthy P, “Feature level fusion of palm print and iris”, IJCSI, ISSN: 1694,-Vol.9, Issue-4, No.1,2012.

[3] Mohamed Abdolahi, Majid Mohamadi and Mehdi Jafari, “Multimodal biometric system fusion using fingerprint, iris with fuzzy logic”, IJSCE, ISSN:2231-2307, Vol-2, Issue-6, 2013.

[4] Velmurugan, S & Selvarajan, S 2018, “A Multimodal Authentication for Biometric Recognition System Using Hybridi Fusion Techniques‘, International Journal of Cluster Computing Springer US, ISSN1386-7857, 2018.

[5] Fernando Bernardo, Gladston Moreira, Eduardo Luz, Paulo H.C.Oliveira and Alvaro Gaurda, “Exploring the scalability of multiple signatures in iris recognition using GA on the acceptance frontier search”, IEEE congress on Evolutionary Computation, pp.1843-1847,2017.

[6] Mohammed Hamzah abed, “Iris recognition model based on Principal Component analysis and 2 level Haar wavelet transform: Case study CUHK and UTIRIS iris databases”, pp-485-500, 2017.

[7] Deepanshu Kumar, Mahati Sastry, Manikantan K, Iris Recognition using Contrast Enhancement and Spectrum-based Feature Extraction, international Conference on Emerging Trends in Engineering, Technology and Science, (2016) 1-7.

[8] Serestina viriri and Jules tapoma, “Iris pattern recognition based on cumulative sums and majority vote methods”, International Journal Advanced Robotics systems, DOI: 10.1177/1729881417703931, 2017

[9] Aparna Gale, G &, Suresh Salankar, S 2016, ‘Evolution of performance analysis of Iris recognition system by using hybrid methods of feature extraction and matching by hybrid classifier for iris recognition system’, International Conference on Electrical, Electronics,and Optimization Techniques (ICEEOT).

[10] CASIA V.4 Iris Image Database Version Three. Available:http://www.cbsr.ia.ac.cn.

[11] CASIA. http://biometrics.idealtest.org

[12] Kalka, ND, Zuo, J, Schmid, NA & Cukic, B 2010, ‘Estimating and Fusing Quality Factors for Iris Biometric Images’, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,vol. 40, pp. 509-524.

[13] Sun, Z, Zhang, H, Tan, T & Wang, J 2014, ‘Iris Image Classification Based on Hierarchical Visual Codebook’, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36, pp. 1120-1133.

[14] Yongqiang, LI. Iris Recognition Algorithm based on MMC-SPP International Journal of Signal Processing, Image Processing and Pattern Recognition 8(2) (2015) 1-10.

[15] Vani Rajasekar, J.Premalatha, K.Sathya, "An efficient signcryption scheme for secure authentication using hyper elliptic curve cryptography and Keccak hashing", International Journal of Recent technology and Engineering (IJRTE), Vol.8, Issue-3, ISSN: 2277-3878, pp: 1593-1598.

[16] Daugman, J 2009, 'Iris Recognition at Airports and Border-Crossings. Encyclopedia of Biometrics', ed: Springer, pp. 819-825.

[17] Zhou, S & Sun, J 2013, 'A Novel Approach for Code Match in Iris Recognition', IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS), pp. 123-128.

[18] A. Poursaberi and B. N. Araabi, "Iris recognition for partially occluded images: Methodology and sensitivity analysis,"Eurasip Journal on Advances in Signal Processing, vol. 2007,Article ID 36751, 2007.

[19] Galbally, J.; Ortiz-Lopez, J.; Fierrez, J.; Ortega-Garcia, J. Iris liveness detection based on quality related features. In Proceedings of the 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 271–276.

[20] Burak Kürşat Gül & Çetin Kurnaz 2016, 'The impact of coding and noise on iris recognition system performance', 24th Signal Processing and Communication Application Conference (SIU).

[21] Daugman, J 2004, 'How Iris Recognition Works', IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 21-30.

[22] Neda Ahmadi, GholamrezaAkbarizadeh, "Hybrid robust iris recognition approach using iris image preprocessing, two dimensional gabor features, and multi layer perceptron neural network/PSO", IET Biometrics, ISSN: 2047-4938, Vol.7, Issue-2, pp. 153-162, 2017.

[23] Ch SA, Nizamuddin N, Sher M (2012) Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In: Information systems, technology and management, communications in computer and information science, vol 285. Springer Berlin Heidelberg, pp 135–142

[24] Inmaculada Tomeo-Reyes, Arun Ross, Antwan Clark, D, Vinod Chandran 2015, 'A biomedical approach to Iris normalization', International Conference on Biometrics (ICB), pp. 9-16,DOI: 10.1109/ICB.2015.7139041

[25] Nizamuddin, Ch SA, Nasar W and Javaid Q 2015 An Efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography, Multimedia Tools Appl pp.1711-1723, DOI 10.1007/s11042-014-2283-9.